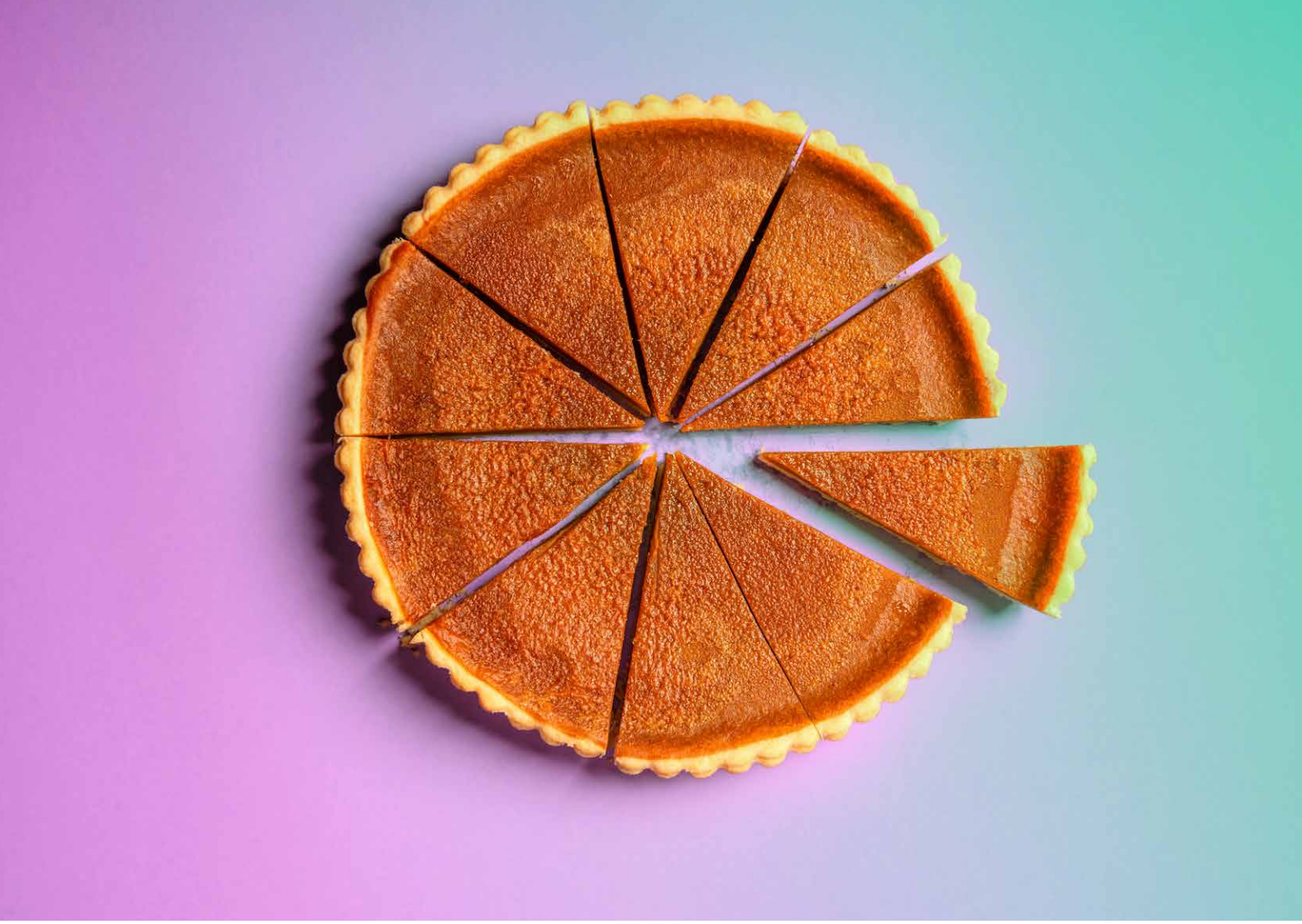


Ajuste dos investimentos: alinhando os orçamentos de TI com as prioridades de segurança em transformação

Economia da segurança de TI de 2020: resumo executivo

kaspersky BRING ON THE FUTURE

Saiba mais em kaspersky.com

Índice

Introdução	2
O custo mutável das violações de dados	4
Consolidação dos principais desafios de cibersegurança	8
Realinhamento dos orçamento de segurança de TI	9
Conclusão	11

Introdução

A linha entre risco e recompensa é muito tênue para qualquer empresa. Não mais do que quando se trata da segurança de seu pessoal e dos dados valiosos que eles detêm.

Sendo 2020 um ano de enormes mudanças e incertezas para todas as organizações, grandes e pequenas, nunca foi tão importante para os líderes de negócios examinar as prioridades da segurança de TI e garantir o alinhamento de procedimentos e orçamentos a fim de propiciar a prosperidade e o crescimento. Uma pesquisa recente da Gartner respalda essa tendência, pois prevê que 75% dos CEOs serão pessoalmente responsáveis pelos incidentes de segurança ciber-físicos em 2024.

Durante a última década, por meio da pesquisa contínua da Kaspersky sobre os aspectos econômicos da segurança de TI, observamos grandes mudanças de prioridades em termos de proteção das empresas, juntamente com grandes avanços na educação, na inteligência e nas soluções de cibersegurança. Mas qual é o impacto da maior dependência da tecnologia e da colaboração on-line sobre os gastos e a perspectiva da segurança atual somente ao longo do último ano?

Este primeiro relatório de uma série examina os aspectos econômicos da segurança de TI, investigando as constatações do título da pesquisa deste ano e preparando o terreno para os custos, desafios e mudanças que afetam os tomadores de decisões da segurança de TI. Curiosamente, o tamanho dos orçamentos de segurança de TI permanece relativamente estável em comparação com os dados de 2019, mas sua participação dentro das despesas totais de TI está crescendo. Isso sugere uma posição importante das medidas de cibersegurança no momento em que são tomadas decisões, em termos de manter os sistemas críticos on-line e conseguir proteger pessoas e dados.

Metodologia

A Pesquisa de Riscos Globais de Segurança Corporativa de TI da Kaspersky (ITSRS) está em seu décimo ano.

Um total de 5.266 tomadores de decisões de negócios de TI de 31 países foram entrevistados em junho de 2020. Os participantes responderam a perguntas sobre o estado da segurança de TI em suas organizações, os tipos de ameaças que enfrentam e os custos incorridos ao recuperar-se de ataques.

Ao longo de todo o relatório, as empresas são classificadas em PMEs (pequenas e médias empresas, com 50 a 999 funcionários) ou grandes corporações (empresas com mais de 1.000 funcionários). Nem todos os resultados da pesquisa estão incluídos neste relatório.

Observe que, embora tenhamos nos empenhado em tornar os resultados dos vários anos comparáveis, a pesquisa passou por mudanças em 2020; por isso, nem todos os resultados podem ser comparados diretamente. O público-alvo permaneceu igual, mas as perguntas de triagem foram revisadas para identificar de modo mais confiável as pessoas com experiência e insights mais relevantes. Isso aumentou significativamente a proporção de respondentes com funções de TI e segurança de TI, de 33% em 2019 para 62% em 2020.

Além disso, embora o escopo do estudo continue sendo global, foram incluídos menos países em 2019 (em especial, a China ficou ausente). A pesquisa de 2020 apresenta uma base de países mais ampla (como em 2018 e 2017) e também inclui Polônia e Cazaquistão na lista.

Principais resultados

Custo das violações de dados

US$ 101 mil
para PMEs

US$ 1,09 milhão
para grandes corporações

Orçamento de segurança de TI

US$ 275 mil
para PMEs

US$ 14 milhões
para grandes corporações

- O custo médio das violações de dados diminuiu para US$ 101 mil para PMEs e US$ 1,09 milhão para grandes corporações em 2020, em comparação com os US$ 108 ml e US$ 1,41 milhão, respectivamente, em 2019
- A participação da segurança de TI no total dos orçamentos de TI cresceu de 23% em 2019 para 26% em 2020 nas PMEs, e de 26% em 2019 para 29% em 2020 nas grandes corporações
- Isso ocorre apesar do menor gasto, de US$ 4,9 milhões para grandes corporações (de US$ 18,9 milhões em 2019 para US$ 14 milhões em 2020) e do leve aumento nos gastos de PMEs, de US $ 8 mil (de US$ 267 mil em 2019 para US$ 275 mil em 2020)
- Três anos atrás, um terço dos tomadores de decisões (33% nas PMEs e 35% nas grandes corporações) admitiu que levava vários meses para se detectar uma violação de dados. Em 2020, esse número caiu drasticamente para apenas 13% das empresas
- Os principais desafios que preocupam as equipes de segurança de TI neste ano são muito específicos: ataques de phishing sobre os clientes (50% das PMEs e 48% das grandes corporações) e ataques sobre filiais (44% das PMEs e 42% das grandes corporações)
- Os maiores determinantes para reduzir os gastos com segurança de TI incluem o fato de um terço (32%) da alta direção das grandes corporações não ver motivo para investir tanto no futuro, e de 29% das PMEs reduzirem as despesas gerais e otimizar os orçamentos da empresa

O custo mutável das violações de dados

Um dos principais fatores determinantes e motivadores de se investir em segurança de TI é, em última análise, o custo para a empresa se isso não acontecer e ocorrer uma violação de dados. Há inúmeros exemplos de empresas que colocam os clientes e sua própria reputação em risco ao sofrer uma violação de dados.

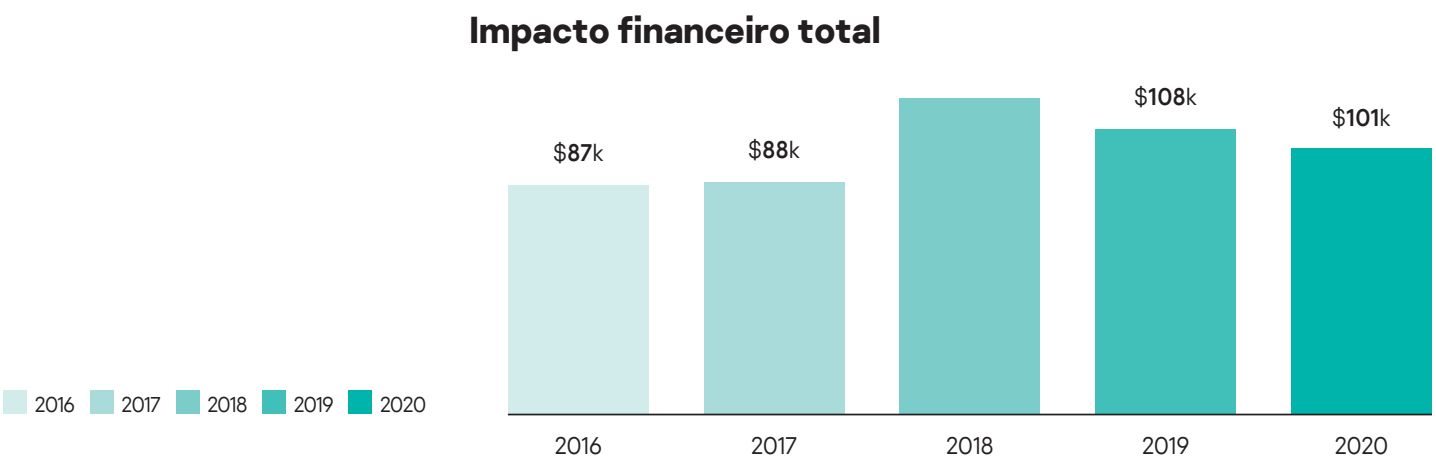
A invasão ocorrida em maio de 2020 direcionada à Blackbaud – um dos maiores provedores do mundo de software de gerenciamento financeiro, arrecadação de fundos e administração da educação – afetou mais de dez universidades no Reino Unido, EUA e Canadá, que tiveram dados de estudantes e ex-alunos roubados depois que hackers atacaram um provedor de computação em nuvem. A cadeia de hotéis Marriot passou novamente por uma violação de segurança em março de 2020, e hackers conseguiram os dados de mais de 5,2 milhões de hóspedes dos hotéis ao longo de um mês, até que a violação fosse descoberta.

Além do efeito danoso sobre a confiança do consumidor e da mancha em suas reputações, essas empresas e muitas outras como elas sofreram enormes custos financeiros e implicações associadas com as violações de segurança, o que pode tornar sua recuperação ainda mais difícil, especialmente no caso de empresas menores, com orçamentos menores e recursos limitados.

A boa notícia é que nossa pesquisa mostrou que o custo de uma violação de dados está caindo, tanto para PMEs quanto para grandes corporações, embora o impacto financeiro ainda esteja aumentando no setor de serviços financeiros, talvez por causa da natureza fortemente regulamentada do segmento e da maior amplitude das consequências da não conformidade.

O impacto financeiro médio de uma violação de dados em PMEs que sofreram pelo menos uma violação de dados fica em US$ 101 mil (em comparação com US $ 108 mil em 2019) e, em grandes corporações, isso chega a US$ 1,09 milhão (em comparação com US$ 1,41 milhão em 2019). Para todas as empresas, os três maiores custos citados que formam este número geral são salários de pessoal interno adicional, perda de negócios e a necessidade de empregar profissionais externos para resolver a violação de dados depois que ela ocorre.

Gráfico 1: Média do impacto financeiro total de uma violação de dados em PMEs



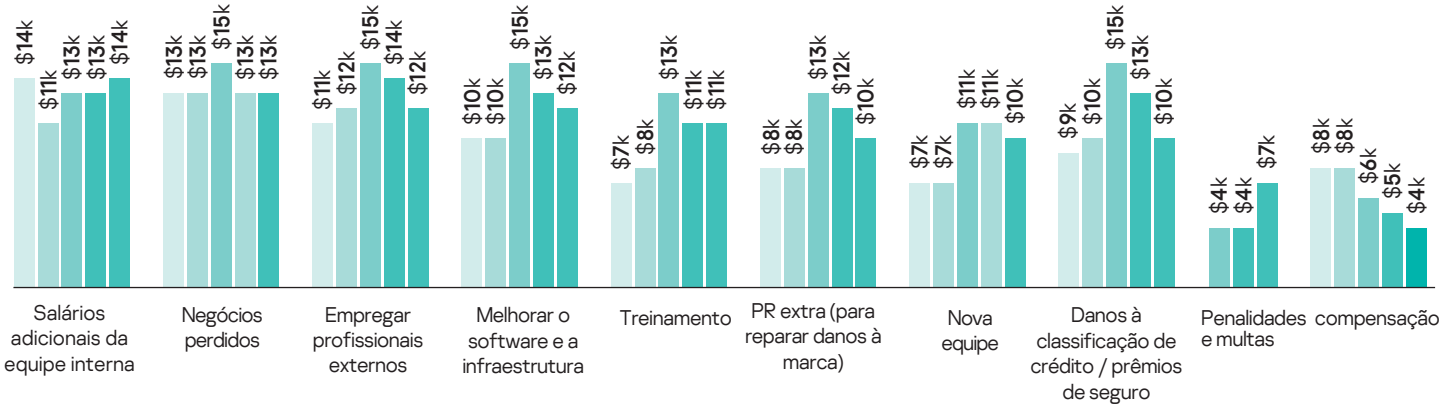
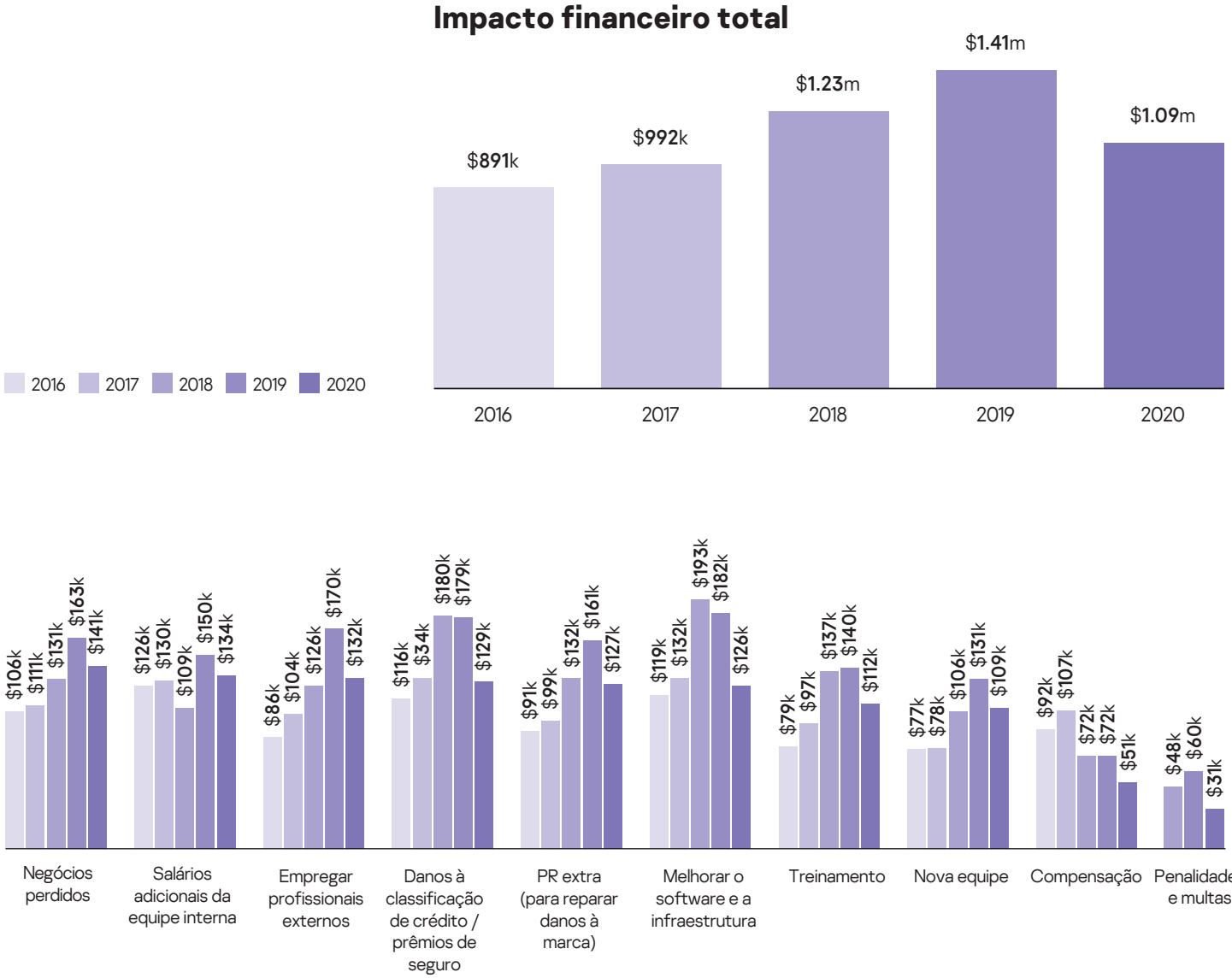


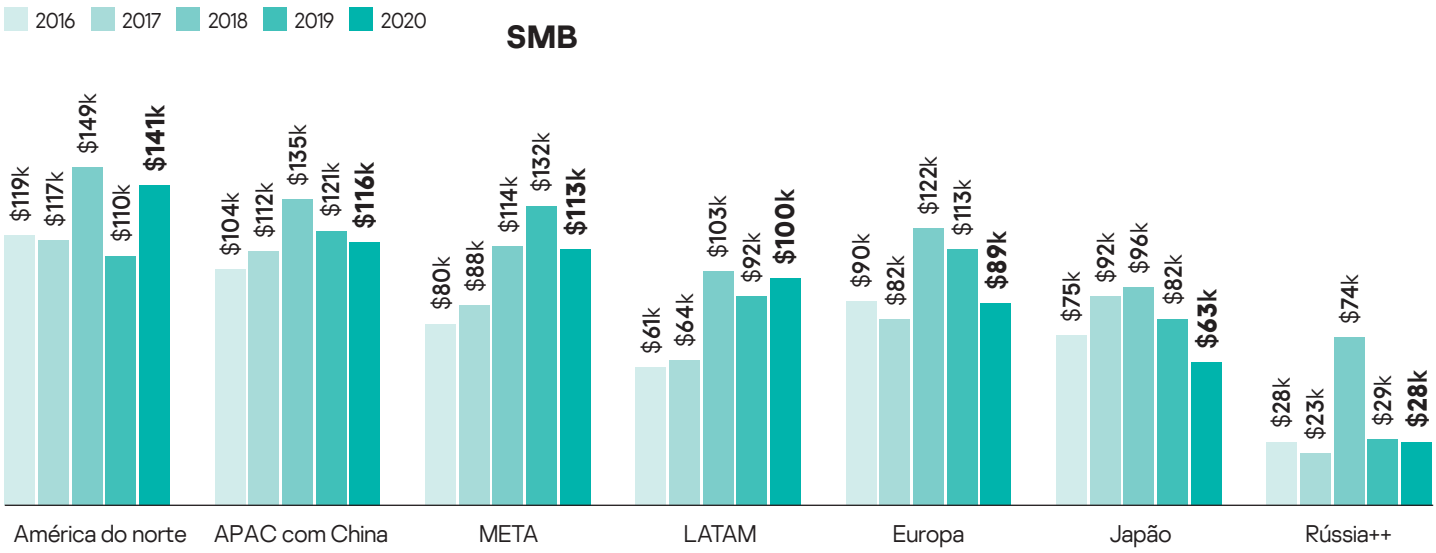
Gráfico 2: Média do impacto financeiro total de uma violação de dados em grandes corporações

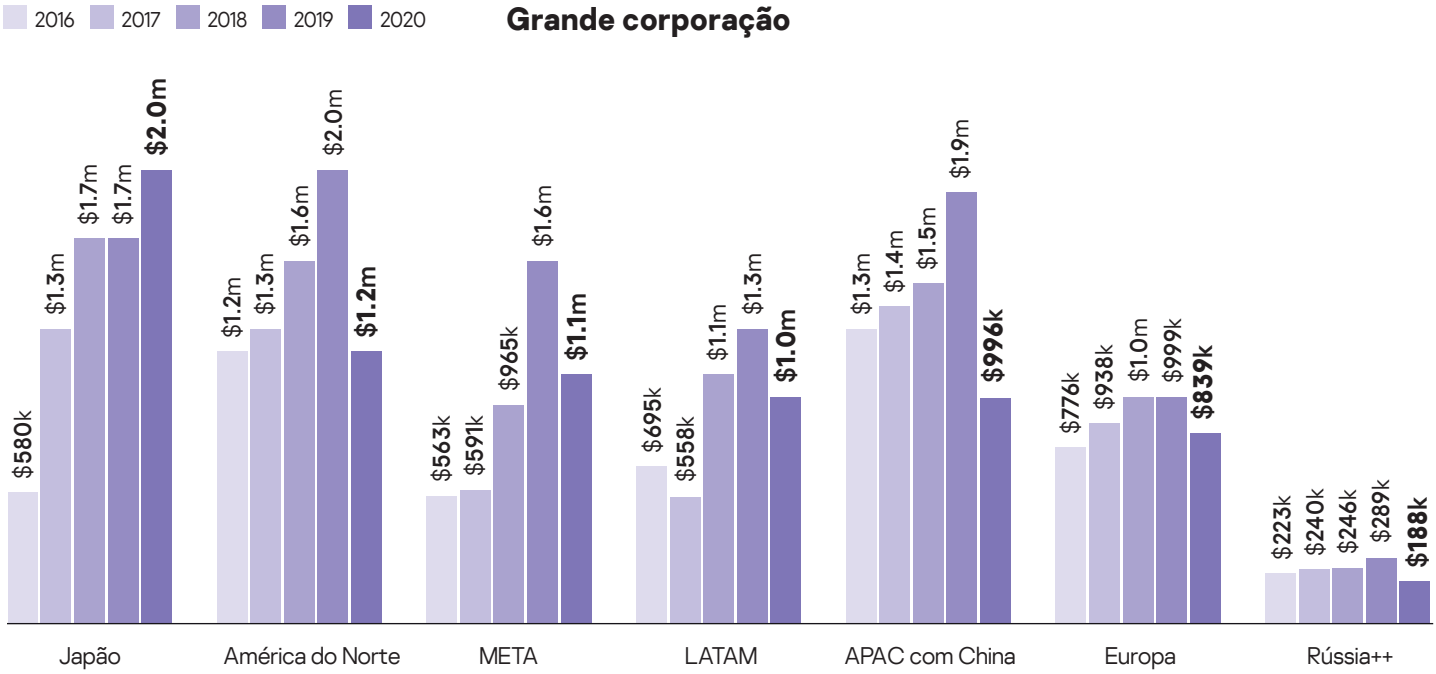


Variações regionais

A maioria das regiões do mundo segue um padrão semelhante em termos da diminuição dos custos associados com uma violação de dados em 2020, com exceção da América do Norte e da América Latina, onde os custos entre PMEs aumentaram, e do Japão, onde o impacto financeiro aumentou para as grandes corporações.

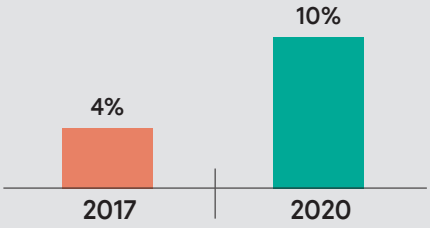
Gráfico 3: Impacto financeiro médio de uma violação de dados nas várias regiões





O valor das reações rápidas

Empresas que detectam ataques quase instantaneamente



Um dos principais motivos para este declínio constante dos custos no mundo inteiro poderia ser as melhorias feitas na detecção de ataques e, portanto, a minimização do impacto das violações sobre as empresas. Nossa pesquisa mostrou que os setores de PMEs e de grandes corporações observaram uma redução significativa no tempo necessário para detectar e reagir a violações de dados ao longo dos últimos anos.

Em 2017, apenas 4% das empresas tinha um sistema funcionando, como uma solução de detecção e resposta nos endpoints ou de prevenção de invasões da rede, capaz de alertá-las sobre uma violação quase instantaneamente. Hoje, esse número aumento para uma a cada dez (10%). Em 2017, um terço dos tomadores de decisões (33% nas PMEs e 35% nas grandes corporações) admitiu que levava vários meses para se detectar uma violação. Em 2020, esse número caiu drasticamente para apenas 13% das empresas.

Ao longo dos últimos três anos, as empresas mudaram a maneira como respondem e reagem à segurança de dados e perceberam o valor de investir seu orçamento em soluções de detecção e resposta, em vez de reagir e pagar somente depois que a violação aconteceu.

Consolidação dos principais desafios de cibersegurança

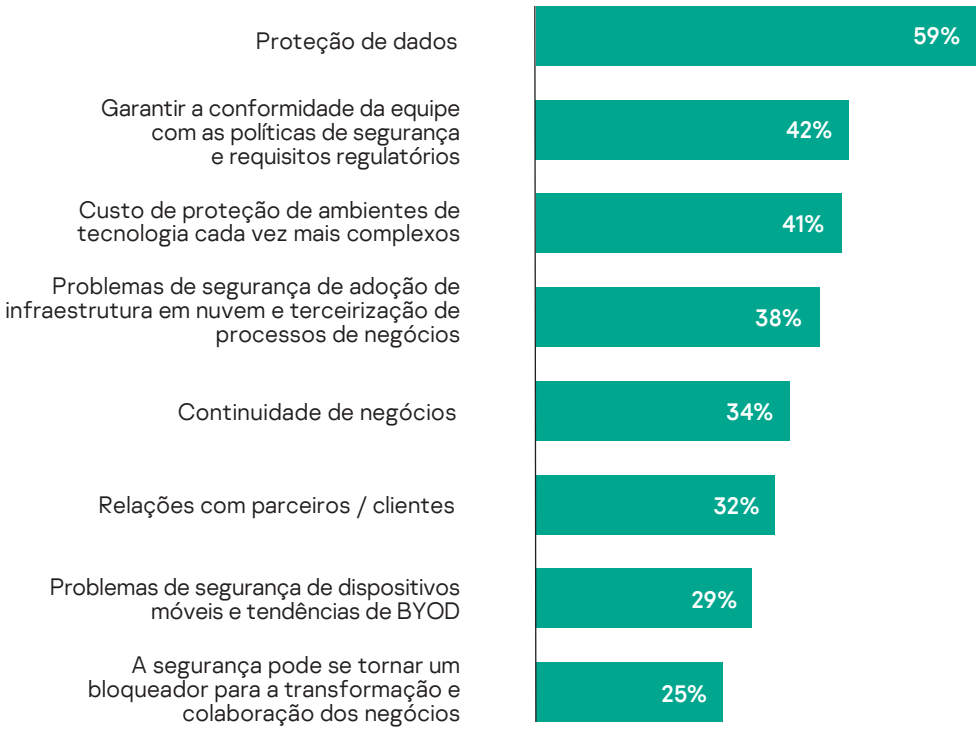
Para todas as empresas, os três problemas de segurança de TI mais preocupantes continuam inalterados nos últimos 12 meses. Proteção de dados (59%), garantir a conformidade com políticas de segurança e regulamentações do setor (42%) e o custo de proteger ambientes tecnológicos cada vez mais complexos (41%) são as principais preocupações dos tomadores de decisões.

No ambiente de COVID-19 atual, não surpreende que essas preocupações continuem no alto da lista de preocupações. Em todo o mundo, empresas mudaram seus modelos de operação e equipes inteiras passaram a trabalhar em casa, o que impôs um a tensão adicional sobre as empresas para garantir que seus sistemas estejam protegidos e em conformidade, e que seus ambientes de TI dispersos permaneçam seguros. Com mais pessoas trabalhando remotamente e fora do relativo conforto e segurança de um ambiente de escritório, também há um ônus sobre as pessoas para continuarem agindo responsavelmente ao usar dispositivos pessoais e de trabalho.

Quando detalhamos preocupações de cibersegurança específicas, obtemos alguns insights muito importantes sobre as mudanças das preocupações. Os ataques de phishing e engenharia social sobre contas de clientes é o maior desafio mencionado por metade das PMEs (50%) e grandes corporações (48%). Eles são seguidos de perto por questões relacionadas a ataques a filiais (44% das PMEs e 42% das grandes corporações).

A pandemia sem dúvida teve um papel na promoção e, aliás, na confirmação desses medos. Nossos especialistas descobriram que os ataques se tornaram mais direcionados e usaram abordagens mais diversificadas durante o período da pandemia.

Gráfico 4: Maiores preocupações com a segurança de TI para todas as empresas



Classificação da preocupação			
2017	2018	2019	2020
1st	1st	1st	1st
5th	3rd	2nd	2nd
4th	6th	3rd	3rd
2nd	2nd	5th	4th
3rd	5th	4th	5th
6th	4th	6th	6th
7th	7th	7th	7th
N/A	N/A	8th	8th

Realinhamento dos orçamento de segurança de TI

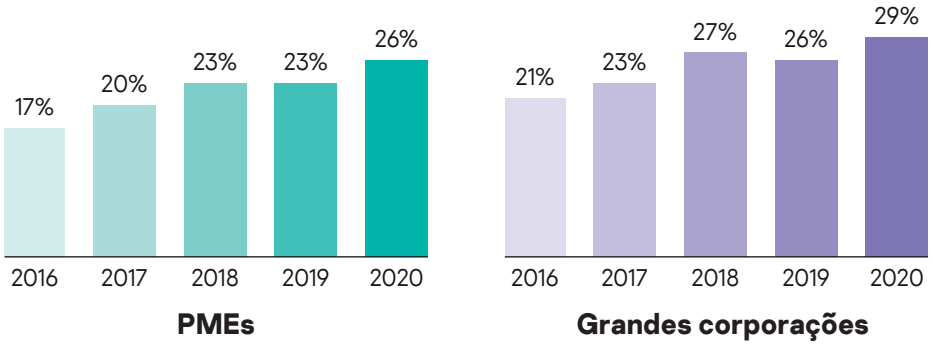
Planejar um orçamento pode ser uma dificuldade para muitas empresas, com a participação de prioridades e parâmetros mutáveis. Quando se trata de alocar gastos de TI, os líderes de negócios já indicaram a paralisação digital e da tecnologia como sua maior prioridade para 2020, segundo a Gartner, mesmo antes da pandemia consolidar-se e a tecnologia tornar-se o principal eixo de quase todas as empresas.

Em 2020, as organizações fizeram mudanças rápidas e significativas em suas operações diárias para poder continuar funcionando e permanecer resilientes face aos desafios em evolução. Dessa forma, vimos os limites de gastos com segurança de TI mudarem ao longo dos últimos 12 meses conforme mudam as prioridades de negócios e os orçamentos disponíveis são ainda mais comprimidos e inspecionados.

Curiosamente, o 'valor' dos orçamentos de segurança de TI continua aumentando, mas não em termos monetários. Como uma parcela do gasto total com TI, a proporção alocada para a segurança está aumentando. Em 2019, 23% do orçamento de TI nas PMEs foi alocado para a segurança, em comparação com 26% em 2020. Nas grandes corporações, esse percentual aumentou de 26% para 29% ao longo dos últimos 12 meses. Porém, quando examinamos os números específicos, os orçamentos permanecem praticamente estáticos (nas PMEs) ou diminuem (nas grandes corporações). Essas constatações estão em grande sincronia com os números recentes da Gartner, que sugerem que os gastos globais de TI diminuirão 8% em 2020 devido ao impacto da pandemia da COVID-19.

Chart 5:

Orçamento de segurança de TI como parcela do orçamento de TI total



	PMEs 2018	PMEs 2019	PMEs 2020	Grandes corporações 2018	Grandes corporações 2019	Grandes corporações 2020
Orçamento de TI médio	$1.1m	$1.2m	$1.1m	$42.1m	$74.1m	$54.3m
Orçamento de segurança de TI médio	$256k	$267k	$275k	$10.2m	$18.9m	$14.0m
Crescimento esperado do orçamento de segurança de TI (ao longo de três anos)	+14%	+11%	+12%	+15%	+11%	+11%

Prioridades de investimento

Mais de dois terços (71%) das PMEs e grandes corporações planejam aumentar os investimentos em segurança de TI ao longo dos próximos três anos, enquanto 17% pretendem mantê-los inalterados. Para as PMEs que esperam aumentar seus gastos com segurança, um dos três principais motivadores citados foi a resposta a maior complexidade das infraestruturas de TI (43% em comparação com 36% no ano anterior). Em sincronia com as constatações já apontadas do relatório, isso é seguido da necessidade de melhorar o conhecimento dos especialistas internos em segurança (39%) e, para um terço (34%) das PMEs, a alta direção deseja aumentar os orçamentos para melhorar as defesas da empresa.

O desejo das grandes corporações de aumentar os orçamentos de segurança mostra uma tendência semelhante. 43% indicam como principais motivos a maior complexidade da infraestrutura de TI, o fortalecimento do conhecimento interno (41%) e o fato da alta direção desejar defesas mais robustas (34%).

Para aquelas que investem em tecnologia em resposta a uma violação de dados, as tecnologias de detecção de rede (46% das grandes corporações e PMEs) e de endpoints (45% das grandes corporações e 41% das PMEs) são seguidas de perto pela inteligência de ameaças tanto em grandes corporações quanto em PMEs (41% e 39%, respectivamente). Isso sugere que as empresas entendem o valor de não apenas reagir rapidamente, mas de ter os insights e as informações necessários para reagir a ameaças que mudam sempre, conforme o cenário cibernético continua evoluindo.

Em contraste com as que esperam investir mais em segurança de TI, 9% das PMEs e 11% das grandes corporações indicaram que planejam reduzir seus orçamentos nessa área nos próximos três anos. O maior motivo para isso, especialmente visível nas grandes corporações, é a sensação de que já foram feitos investimentos suficientes para proteger a organização e que não é necessário manter os níveis atuais de investimento.

Por exemplo, um terço (32%) da alta direção de grandes corporações não vê motivos para investir tanto em segurança de TI, o principal argumento fornecido para reduzir orçamentos. Um quarto das PMEs (25%) acredita estar suficientemente segura e não precisar gastar mais nesta área, mas o principal motivo para reduzir os investimentos é a redução global de despesas da empresa e a otimização geral do orçamento (29%).

Gráfico 6: Principais motivos para reduzir investimentos em segurança de TI

Motivos apresentados para esperar uma redução nos gastos com segurança de TI durante os próximos três anos	PME		Grande corporação	
	%	Classificação	%	Classificação
Cortes globais de despesas da empresa/otimização geral do orçamento	29%	1	26%	5
Grandes investimentos nos últimos anos resolveram problemas importantes, agora é necessária apenas uma manutenção	25%	3	30%	2
A alta direção não vê motivo para investir tanto em segurança de TI	23%	5	32%	1
Somos suficientemente seguros e não é necessário investir mais em segurança de TI	25%	2	22%	7
A terceirização de algumas funções de segurança de TI nos permite reduzir custos	22%	7	26%	4
Orçamento de TI realocado para outras necessidades da empresa	19%	8	27%	3
Devido à diminuição dos negócios	23%	4	20%	10
Não houve incidentes de segurança nos últimos 12 meses	22%	6	21%	8
Mudou para uma solução/fornecedor de proteção de endpoints mais barato	19%	8	23%	6
Demanda de nossos acionistas e investidores	15%	10	21%	9

Conclusão

Apesar os eventos únicos que ocorreram em 2020, nossa pesquisa identificou diversas tendências recorrentes e sugere uma perspectiva positiva para a priorização da segurança de TI e investimentos maiores nesta área, tanto nas comunidades de PMEs quanto de grandes corporações.

Sem dúvida, o menor impacto financeiro de uma violação de dados sobre as empresas é uma ótima notícia que sugere que a maior parte das medidas de redução estão funcionando e que os orçamentos estão sendo investidos nos lugares certos.

Porém, os números não devem indicar complacência, mas servir como comprovação de que medidas de segurança de TI intensas e robustas funcionam e são fundamentais para possivelmente economizar a longo prazo. A crescente parcela da segurança de TI nas despesas gerais de TI indica o valor depositado em medidas de segurança e, com certeza, é uma área que as empesas devem continuar ampliando para manter os mais altos níveis de segurança e proteção em meio a um cenário de ameaças que muda continuamente.

É claro que a adesão e a compreensão da alta direção são fundamentais para garantir e efetivamente aumentar os investimentos, especialmente dentro de grandes corporações. Mesmo nos casos em que os respondentes mencionaram orçamentos reduzidos nos próximos anos, o investimento e desenvolvimento de infraestruturas de cibersegurança até o momento foram extremamente positivos. O reconhecimento, a inteligência e a reação definitiva a ameaças evoluíram em conjunto com o desejo de qualificar e reforçar as equipes internas de segurança.

Como forma de vigilância proativa, deve haver uma conscientização sobre como o trabalho remoto e as equipes mais dispersas aumentam os níveis de vulnerabilidade das empresas. Basta observar a rápida evolução das táticas de engenharia social, inclusive o phishing, para ver como os cibercriminosos continuam aprimorando seu arsenal de ataque e mantendo as equipes de TI em alerta.

Para ajudar as empresas a resolver estes desafios contínuos e garantir que orçamentos e ações estejam alinhados com as prioridades atuais e as ameaças dinâmicas, a Kaspersky sugere as seguintes medidas:

- Ao planejar seu orçamento de cibersegurança, use uma abordagem baseada em riscos. Examine as ameaças mais relevantes ao seu setor e ao tamanho de sua empresa; depois, considere o custo para a empresa e a probabilidade de ocorrência do risco ao priorizar o que deve ser resolvido primeiro
- A terceirização pode ser uma boa opção para organizações que não têm o conhecimento interno necessário ou processos de avaliação de riscos. Firmar um contrato de nível de serviço (SLA) garantido em qualquer terceiro e transferir despesas de CapEx para OpEx é uma forma de manter os gastos com segurança sob controle
- Forneça treinamento básico em higiene de cibersegurança para toda a sua equipe. Aprimore as habilidades de seus funcionários de segurança de TI continuamente para que eles consigam defender você até de ataques sofisticados. Por exemplo, a Kaspersky oferece treinamento on-line em busca de ameaças com regras da YARA
- Apesar do custo de violações de dados estarem diminuindo ano a ano, as empresas devem continuar vigilantes e sempre usar uma solução de cibersegurança dedicada, que associem proteção de endpoints com funcionalidades de detecção. A solução de segurança integrada de endpoints da Kaspersky oferece visibilidade instantânea e insights de incidentes, juntamente com opções imediatas de investigação e resposta automatizada
- As soluções de segurança que podem ser gerenciadas na nuvem devem simplificar a proteção de escritórios remotos e filiais, outra preocupação importante dos especialistas em cibersegurança neste ano
- Garanta a proteção contra spam e phishing para que agentes maliciosos não consigam tirar proveito da credulidade dos funcionários, seja associada à COVID-19 o a qualquer outro evento ou tendência. Isso também é relevante para serviços de e-mail SaaS, como o Microsoft Office 365
- Para proteger clientes de phishing, ensine a eles os possíveis truques que os criminosos usam. Envie informações regularmente a eles sobre como identificar fraudes e quais ações devem ser realizadas nessas situações. Caso alguém assuma o controle da conta de um cliente, uma solução antifraude capaz de detectar anomalias e comportamento suspeito do usuário será extremamente valiosa

Para obter mais insights sobre os custos cambiantes associados com a segurança de TI e como manter sua empresa protegida de ameaças dinâmicas e violações de dados, siga #securityeconomics para obter nossa série de relatórios sobre o assunto.

Notícias sobre ameaças cibernéticas: securelist.com
Notícias sobre segurança de TI: business.kaspersky.com

kaspersky.com

kaspersky

GBD-7018 Q3/20 V1